Лабораторная работа «Исследование сетевых протоколов»

Вопросы

1. Опишите формат IP- датаграммы. Какой размер имеет стандартный IP – заголовок.
2. Какие поля используются для управления фрагментацией. Как изменяется поле «время жизни»
3. Пакеты каких протоколов сетевого уровня встречались среди перехваченных пакетов. Какие из них являются маршрутизируемыми, а какие нет.
4. Опишите формат пакета протокола DHCP и типы передаваемых сообщений.
5. Опишите формат пакета протокола ICMP. Какие типы сообщений вам встречались. Какие занчения “тип” и “код” сообщения они имеют.
6. Опишите работу утилит ping и traceroute. Их отличие. Чем отличаются несколько последовательных echo-запросов.

7. Опишите формат пакета протокола ARP. Какие значения полей устанавливает отправитель в ARP-запросе и получает в ARP-ответе.
8. Опишите формат фрейма Ethernet. Какая версия технологии Ethernet используется в вашей сети.
9. Какой MAC-адрес имеет сетевая карта вашего компьютера и какой у маршрутизатора сети.
10. Опишите формат сообщения TCP. Какой номер протокола соответствует TCP.
11. Опишите последовательность установления соединения. Какие параметры при этом необходимо синхронизировать сторонам. Какие номера последовательностей имеют первые пакеты соединения.
12. Опишите механизм управлением соединением TCP. Какие поля используются для подтверждения приема сегментов. Опишите алгоритм управления размером окна в TCP.

13. Опишите формат пакета UDP. Какой максимальный размер может иметь UDP- пакет. Какой номер протокола соответствует UDP.
14. Какие номера UDP- и TCP- портов встречались в работе. По каким признакам могут различаться потоки разных приложений
15. На примерах перехваченных пакетов опишите работу системы DNS. Какой из протоколов (TCP или UDP) использует DNS. Какие номера портов имеют сообщения DNS.
16. Перехватите соединение с Web-сервером и восстановите сообщения, содержащие запрос и ответ, а также другие файлы, передаваемые в рамках данного соединения.

Задания по IP-адресации

17. Для некоторого IP -адреса хоста найдите адрес сети и широковещательный адрес (например, 172.16.210.0/22, 201.100.5.68/28, 172.16.209.10/22).
18. Какие из указанных адресов могут быть присвоены хостам в сети, к которой принадлежит адрес 192.168.15.19/28
    (192.168.15.17, 192.168.15.14, 192.168.15.29, 192.168.15.16, 192.168.15.31)
19. Какие из указанных адресов могут быть присвоены хостам в сети с маской 255.255.255.224
    (16.23.118.63, 87.45.16.159, 92.11.187.93, 134.178.18.56, 192.168.16.87, 217.168.166.192)
20. Есть сеть класса C которую необходимо разделить как минимум на 10 подсетей с максимально возможным числом хостов. Какую маску подсети вы будете использовать?.
21. Сколько подсетей и с каким количеством хостов получится, если разделить маской /28 сеть 210.10.2.0.
22. Необходимо разделить одну сеть организации класса C на подсети отделов , в которых будет работать соответственно 15, 13, 7 и 16 станций. Какая маска дает возможность произвести такое разделение, чтобы в каждой подсети было достаточное количество адресов.

1. ОСНОВЫ ЗАХВАТА И АНАЛИЗА СЕТЕВОГО ТРАФИКА

Мониторинг и анализ сетевого трафика являются неотъемлемой частью процесса управления компьютерной сетью и используются для диагностики, тестирования и поиска неисправностей, для оптимизации структуры информационных потоков, а также выявления и решения проблем в обеспечении безопасности узлов компьютерной сети и информации, циркулирующей между ними.

Целью данного занятия является приобретение навыков захвата сетевого трафика в сегменте локальной сети и анализа собранной информации с помощью программного анализатора протоколов Ethereal. Для успешного достижения целей занятия слушателям необходимо повторить теоретический материал, касающийся назначения и функционирования протоколов стека TCP/IP.

Для изучения материала данной главы в учебном классе должен быть развернут сегмент локальной вычислительной сети на концентраторе или коммутаторе, включающий в себя рабочие станции с операционной системой Windows 2000/XP по количеству слушателей. При выполнении некоторых упражнений понадобится наличие сервера HTTP или подключение к сети Интернет. Для установки необходимого программного обеспечения на рабочих станциях должны быть доступны инсталляционные пакеты библиотеки WinPCap (версия не ниже 2.3) и анализатора Ethereal (версия не ниже 0.10.11).

1.1. Общие сведения о программе

Существует множество инструментальных средств, предоставляющих необходимые возможности для выполнения мониторинга сети и анализа сетевого трафика. Одним из таких средств является пакет Ethereal, представляющий собой программный анализатор протоколов. Анализатор протоколов переводит сетевой адаптер в режим «беспорядочного» приема кадров, записывает в свой буфер отфильтрованные кадры сетевого трафика, по запросам пользователя выводит на экран те или иные кадры из буфера и посредством декодера протоколов предоставляет пользователю информацию о значениях полей заголовка протокола и содержимое его блока данных.

Как и большинство программ такого класса, Ethereal содержит следующие основные компоненты: фильтр захвата, буфер кадров, декодер протоколов, фильтр отображения захваченных кадров и модуль статистики с элементами экспертной системы. К несомненным достоинствам Ethereal относятся:

- наличие реализаций для Unix и Windows;
- наличие исходного кода программы;
- возможность захвата трафика в сетевых сегментах различных базовых технологий;

− возможность анализа огромного числа протоколов (более 700);
− возможность экспорта/импорта файлов данных в формат распространенных анализаторов (несколько десятков форматов);
− мощная и удобная система поиска и фильтрации информации в буфере пакетов;
− наличие элементов экспертной системы;
− возможность сохранения на диск выделенного фрагмента пакета;
− наличие полезных утилит командной строки для осуществления захвата трафика и обработки сохраненных файлов.

1.2. Установка программы и подготовка к захвату

ВЫПОЛНИТЬ!

1. Установите библиотеку WinPCap и анализатор Ethereal, для чего последовательно запустите соответствующие файлы установки.

Некоторые дистрибутивы Ethereal содержат в себе инсталлятор требуемой версии библиотеки WinPCap.

2. Запустите Ethereal и разверните главное окно приложения на весь экран (для удобства работы).

Перед выполнением захвата сетевого трафика необходимо настроить параметры захвата или проконтролировать установленные значения некоторых из них так, чтобы собранная информация адекватно соответствовала решаемой задаче анализа трафика.

ВЫПОЛНИТЬ!

3. Выполните команду меню ***Capture ⇒ Options***.

В открывшемся диалоговом окне устанавливаются следующие параметры захвата кадров (рис. 1.1):
− Interface — сетевой адаптер;

Очень важно выбрать соответствующий сетевой адаптер, иначе запись кадров будет производиться из другого сегмента сети! В компьютере, имеющем всего один сетевой адаптер, среди возможных сетевых интерфейсов часто присутствует контроллер удаленного доступа!

− Buffer size — размер буфера захвата (по умолчанию 1 Мб);

При малом размере буфера существует опасность того, что при его заполнении запись новых кадров будет производиться поверх записанных ранее!

– Capture packets in promiscuous mode — использование режима беспорядочного захвата.

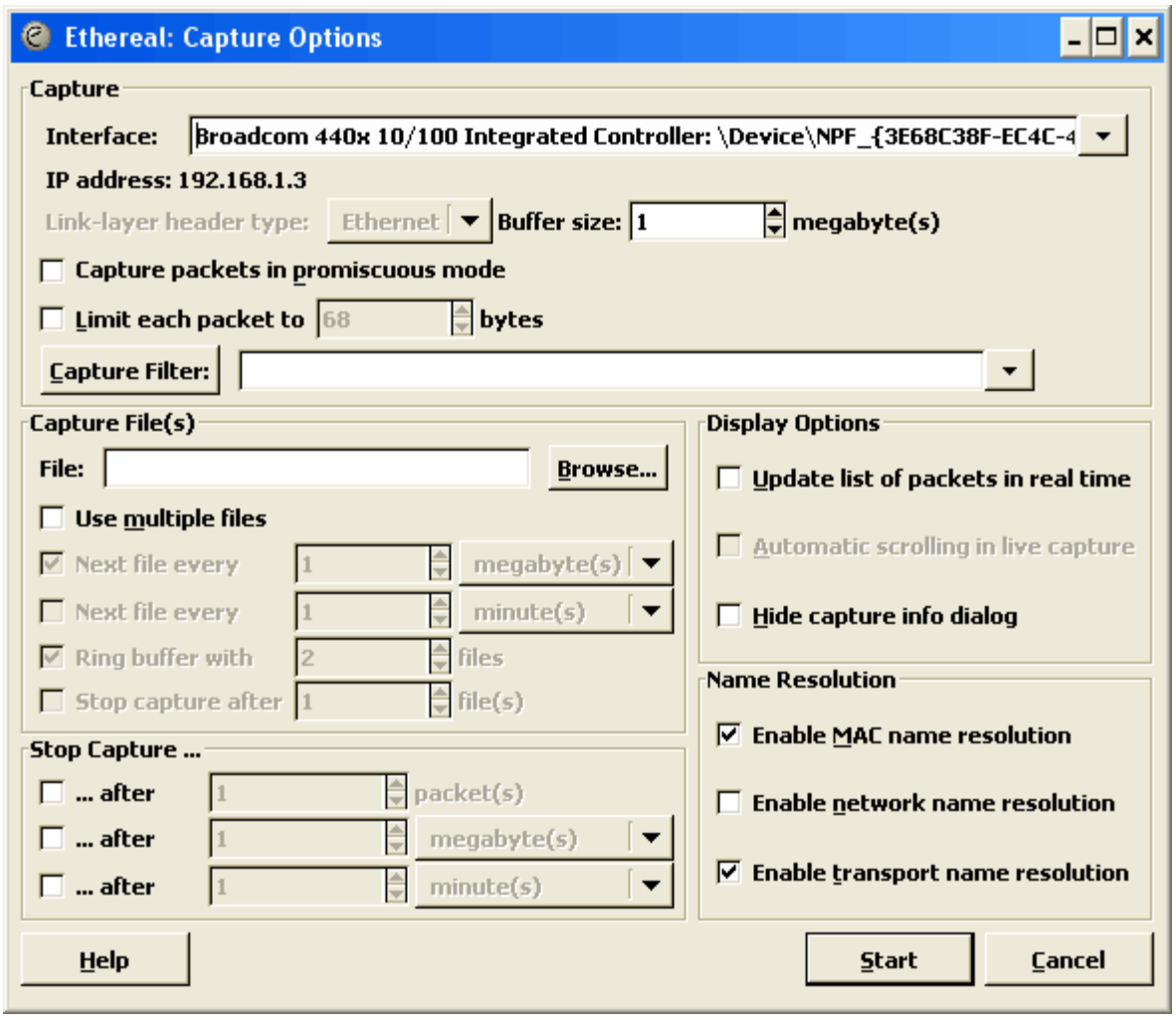


Рис. 1.1. Окно настройки параметров захвата

– Limit each packet to — запись только нескольких первых байт (определяется установленным значением параметра) каждого кадра;

– Capture Filter — фильтр захвата;

Фильтр захвата экономит объем буфера, отбрасывая «лишний мусор», однако увеличивает нагрузку на процессор, вследствие чего некоторые кадры могут быть потеряны. Поэтому в некоторых случаях вместо фильтра записи предпочтительнее использовать фильтр отображения кадров в буфере, а запись производить без фильтрации!

– Capture File(s) — файл захвата;

Опция полезна при осуществлении захвата трафика в течение длительного периода времени.

– Stop Capture — условия автоматического завершения захвата;

− Display Options — отображение пакетов в реальном времени и автоматический скроллинг окна информации;

Опции увеличивают нагрузку на процессор, вследствие чего некоторые кадры могут быть потеряны.

− Name Resolution — разрешение имен на физическом, сетевом и транспортном уровнях.

ВЫПОЛНИТЬ!

4. Уберите маркер напротив опции «Capture packets in promiscuous mode» для захвата только «своих» кадров (кадры с широковещательным адресом также будут захватываться). В таком режиме работы число захваченных пакетов будет существенно меньше, что облегчит выполнение заданий.

1.3. Пользовательский интерфейс программы

ВЫПОЛНИТЬ!

5. В командной строке сеанса MS-DOS для очистки кэша протокола ARP выполните команду `arp -d`. В Ethereal для запуска процесса захвата нажмите кнопку «Capture». В командной строке выполните команду `ping <имя_сервера>` (в качестве параметра команды можно использовать IP-адрес сервера). По завершении команды Ping остановите захват, нажав кнопку «Stop».

На экране монитора в программе Ethereal вы увидите несколько панелей с отображением сетевых пакетов, только что записанных в буфер. Общий вид окна приложения представлен на рис. 1.2. Пользовательский интерфейс программы содержит следующие компоненты:

− меню команд и панель инструментов;
− фильтр отображения пакетов;
− список пакетов в буфере;
− панель отображения декодера протоколов;
− панель отображения пакета в шестнадцатеричном коде и символах ASCII.

Панель со списком пакетов построчно отображает характеристики того или иного пакета (номер по порядку в буфере, время захвата, адреса источника и получателя, тип протокола и общая информация о нем). Перемещение по списку осуществляется с помощью мыши или клавиатуры, причем информация на двух других панелях обновляется автоматически. На панели декодера протоколов, нажимая указателем мыши на символы «+» или «–», можно отображать информацию о полях заголовков протоколов с требуемым уровнем детализации. При выборе того или иного служебного поля в заголовке оно автоматически выделяется на нижней панели, где отображается текущий пакет в шестнадцатеричном виде.

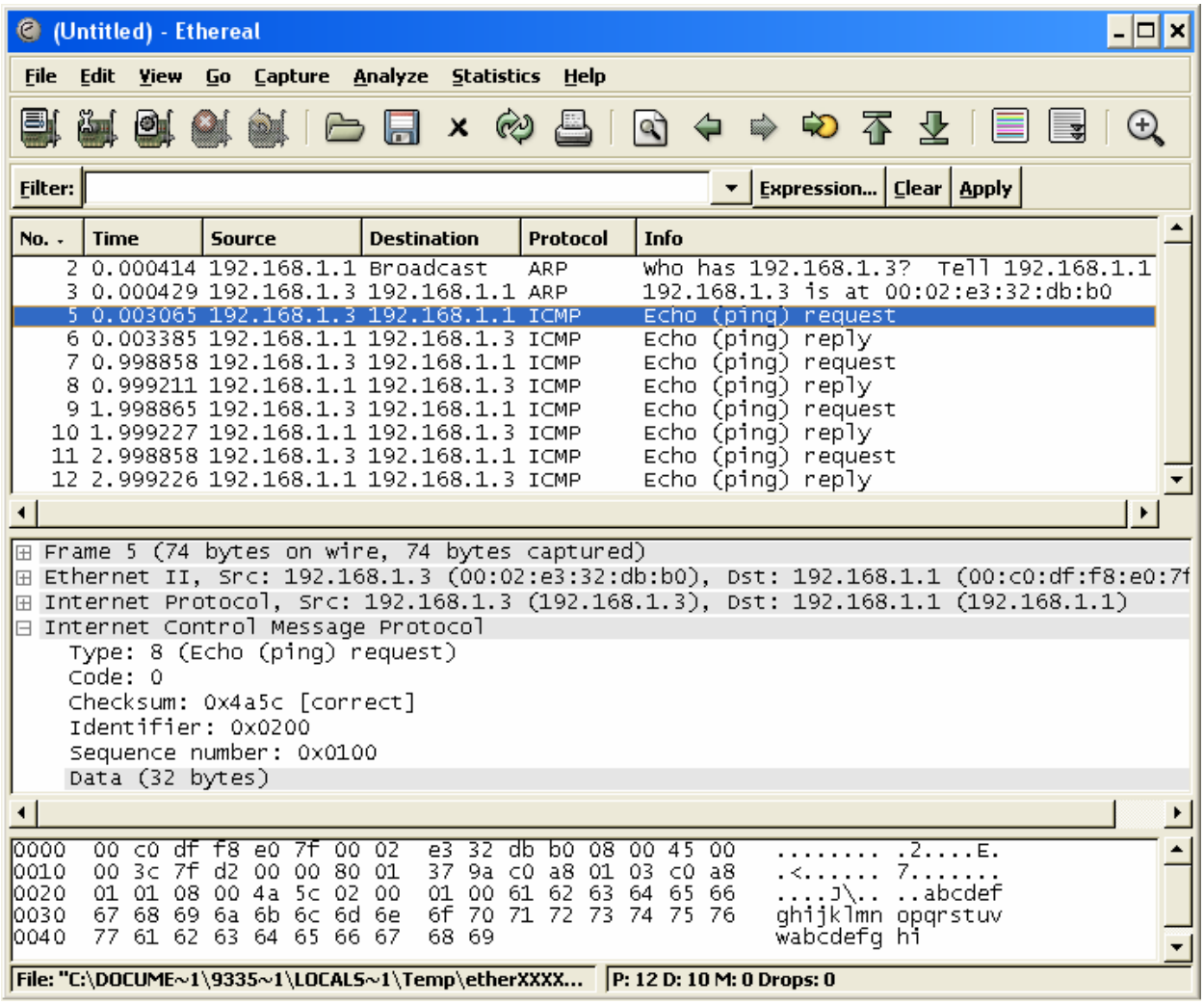


Рис. 1.2. Общий вид приложения Ethereal

1.4. Фильтр отображения пакетов

С помощью фильтра отображения можно быстро убрать «мусор». Выражение фильтрации может представлять собой просто название протокола, который присутствует в пакете на том или ином уровне вложенности. Например: arp — для отображения пакетов протокола ARP, tcp — для отображения пакетов, в которых присутствует заголовок протокола TCP.

ВЫПОЛНИТЬ!

6. Для отображения только ICMP-сообщений в строке ввода «Filter» (рис. 1.2) наберите «icmp» и нажмите кнопку «Apply».

Более сложные выражения фильтрации строятся с помощью зарезервированных слов, обычно представляющих собой названия полей заголовков того или иного протокола, знака операции сравнения и конкретного значения в шестнадцатеричном или десятичном виде. Наиболее часто используемые выражения фильтрации и их значения приведены в табл. 1.1.

Таблица 1.1

Выражения фильтрации и их значения

Выражение	**Значение выражения и пример записи**
frame.marked	Маркированный кадр `frame.marked == true`
frame.number	Номер кадра `frame.number == 150`
frame.time	Время захвата кадра `frame.time == "Feb 1, 2006 09:00:00"`
frame.pkt_len	Длина кадра `frame.pkt_len == 48`
eth.dst	Заголовок Ethernet: MAC-адрес назначения `eth.dst == 01:00:5e:00:00:02`
eth.src	Заголовок Ethernet: MAC-адрес источника `eth.src == 00:a0:cc:30:c8:db`
eth.type	Заголовок Ethernet: тип вложенного протокола `eth.type == 0x0800`
arp.hw.type	Заголовок протокола ARP: тип протокола канального уровня `arp.hw.type == 0x0001`
arp.proto.type	Заголовок протокола ARP: тип протокола сетевого уровня `arp.proto.type == 0x0800`
arp.opcode	Заголовок протокола ARP: код операции `arp.opcode == 0x0001`
arp.src.hw_mac	Заголовок протокола ARP: MAC-адрес источника `arp.src.hw_mac == 00:10:4b:30:c4:4a`
arp.src.proto_ipv4	Заголовок протокола ARP: IP-адрес источника `arp.src.proto_ipv4 == 10.1.0.1`
arp.dst.hw_mac	Заголовок протокола ARP: MAC-адрес назначения `arp.dst.hw_mac == 00:00:00:00:00:00`
arp.dst.proto_ipv4	Заголовок протокола ARP: IP-адрес назначения `arp.dst.proto_ipv4 == 10.1.0.2`
ip.version	Заголовок протокола IP: версия протокола IP `ip.version == 4`
ip.hdr_len	Заголовок протокола IP: длина заголовка `ip.hdr_len == 24`
ip.flags.df	Заголовок протокола IP: флаг фрагментации `ip.flags.df == 0`
ip.flags.mf	Заголовок протокола IP: флаг не последнего фрагмента `ip.flags.mf == 0`

Выражение	Значение выражения и пример записи
ip.frag_offset	Заголовок протокола IP: смещение фрагмента `ip.frag_offset == 0`
ip.ttl	Заголовок протокола IP: время жизни пакета `ip.ttl == 1`
ip.proto	Заголовок протокола IP: протокол вышестоящего уровня `ip.proto == 0x01`
ip.src	Заголовок протокола IP: IP-адрес источника `ip.src == 10.0.0.99`
ip.dst	Заголовок протокола IP: IP-адрес назначения `ip.dst == 224.0.0.2`
ip.addr	Заголовок протокола IP: IP-адрес `ip.addr == 10.2.0.0/16`
tcp.srcport	Заголовок протокола IP: порт источника `tcp.srcport == 1054`
tcp.dstport	Заголовок протокола IP: порт назначения `tcp.dstport == 21`
tcp.seq	Заголовок протокола IP: последовательный номер `tcp.seq == 4856133`
tcp.ack	Заголовок протокола IP: номер подтверждения `tcp.ack == 4856134`
tcp.flags.urg	Заголовок протокола IP: бит присутствия срочных данных `tcp.flags.urg == 0`
tcp.flags.ack	Заголовок протокола IP: бит присутствия подтверждения `tcp.flags.ack == 1`
tcp.flags.push	Заголовок протокола IP: бит выталкивания данных `tcp.flags.push == 0`
tcp.flags.reset	Заголовок протокола IP: бит сброса соединения `tcp.flags.reset == 0`
tcp.flags.syn	Заголовок протокола IP: бит синхронизации сессии `tcp.flags.syn == 1`
tcp.flags.fin	Заголовок протокола IP: бит завершения сессии `tcp.flags.fin == 0`
tcp.window_size	Заголовок протокола IP: размер приемного окна `tcp.window_size == 8760`
udp.srcport	Заголовок протокола UDP: порт источника `udp.srcport == 2364`
udp.dstport	Заголовок протокола UDP: порт назначения `udp.dstport == 53`

Выражение	Значение выражения и пример записи
icmp.type	Заголовок протокола ICMP: тип сообщения `icmp.type == 8`
icmp.code	Заголовок протокола ICMP: уточняющий код сообщения `icmp.code == 0x00`

В примерах записи выражений табл. 1.1 приведены выражения с операцией сравнения «Равно», которая записывается с помощью двойного знака равенства «==» (допустимо использование «eq»). Другие операции сравнения записываются с помощью следующих операторов:

a. `!=` `(ne)` — не равно, пример: `eth.type != 0x0800`;
b. `>` `(gt)` — больше, пример: `tcp.srcport > 1023`;
c. `<` `(lt)` — меньше, пример: `frame.pkt_len lt 60`;
d. `>=` `(ge)` — больше или равно, пример: `frame.pkt_len ge 60`;
e. `<=` `(le)` — меньше или равно, пример: `tcp.dstport <=1023`.

ВЫПОЛНИТЬ!

7. Выясните, что будет отображено в буфере захвата в случае использования фильтра, описанного с помощью выражений, приведенных в качестве вышеописанных примеров.

Значение любого выражения фильтрации возвращает переменную булевского типа. Таким образом, выражение `udp` означает присутствие в кадре заголовка протокола UDP, по аналогии с этим выражение `tcp.flags.syn` означает присутствие в заголовке протокола TCP бита синхронизации сессии в установленном состоянии (значение 1). К любому из выражений можно применить операцию логического отрицания, заключив его в скобки и поставив перед ним знак отрицания «NOT» или «!». Например, выражение `!(ip.addr == 10.0.0.1)` означает, что из буфера отображения необходимо убрать все пакеты, в которых встречается IP-адрес 10.0.0.1.

ВЫПОЛНИТЬ!

8. Объясните разницу между результатами использования выражений фильтрации `!(ip.addr == X.X.X.X)` и `ip.addr !== X.X.X.X`. Для выполнения упражнения в выражениях фильтрации используйте вместо адреса `X.X.X.X` реальный IP-адрес вашего узла.

В качестве выражений фильтрации можно использовать и составные выражения, которые образуются с помощью следующих логических операторов:

a. && (AND) — логическое И,
   пример: `(ip.dst==10.0.0.1) AND tcp.flags.syn`;

b. || (OR) — логическое ИЛИ,
   пример: `(ip.addr==10.0.0.1) OR (ip.addr==10.0.0.2).`

Другой удобный способ ввода выражения фильтрации состоит в следующем. На панели декодера протоколов отображается требуемое поле, в контекстном меню выбирается пункт «Apply as Filter» и далее исполняется либо команда «Selected», либо «Not Selected» в зависимости от задачи фильтрации (рис. 1.3).

ВЫПОЛНИТЬ!

9. Отобразите только ICMP-запросы (используйте поле «тип» в заголовке ICMP). Укажите результирующее выражение фильтрации с необходимыми пояснениями. После просмотра результата для отображения пакетов без фильтрации нажмите кнопку «Clear» в строке фильтра.

При необходимости создания сложного выражения фильтрации в меню «Apply as Filter» (рис. 1.3) выбирайте команды, начинающиеся с многоточия, при этом новое выражение будет добавлено к результирующему выражению фильтрации.

10. Отобразите все кадры, переданные вашим узлом, исключая сообщения ICMP.

При создании выражения фильтрации имейте в виду, что в буфере могут находиться кадры других узлов.

Укажите результирующее выражение фильтрации с необходимыми пояснениями. После просмотра результата для отображения пакетов без фильтрации нажмите кнопку «Clear» в строке фильтра.

В выражениях фильтрации первый операнд операции сравнения допускает использование указателя диапазона, если второй операнд представляет собой массив байт или строку символов. Указатель диапазона определяется с помощью квадратных скобок и может быть использован как применительно к кадру в целом (frame), так и с любым полем заголовка. Указатель диапазона допускает следующий синтаксис:

a. [i:j] начальное смещение i, длина j;
b. [i-j] начальное смещение i, конечное смещение j, включительно;
c. [i] начальное смещение i, длина 1;
d. [:j] начальное смещение 0, длина j;
e. [i:] начальное смещение i, до конца поля.

Например, записи `frame[6:3]` и `eth.src[:3]` идентичны и могут быть использованы для указания на код фирмы-производителя сетевого адаптера, передавшего кадр. Начальное смещение может иметь отрицательное значение, в этом случае оно отсчитывается от конца поля, причем последний байт поля имеет смещение, равное –1, предпоследний –2 и так далее. Напри-

мер, выражение `frame[-5:] == "hello"` определяет кадр, оканчивающийся строкой «hello».

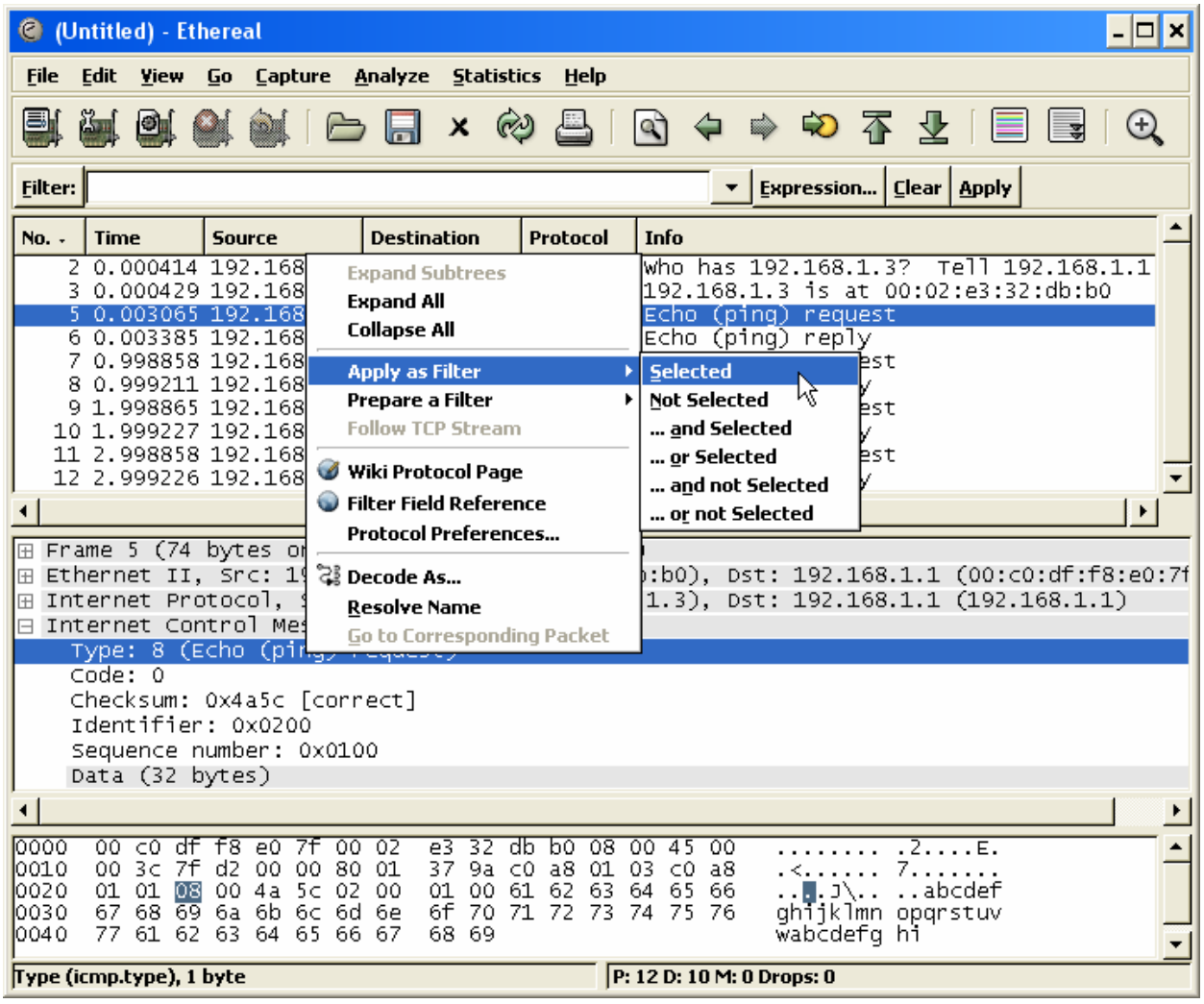


Рис. 1.3. Контекстное меню создания фильтра

Строка, как видно из предыдущего примера, записывается в кавычках. Запись массива байт осуществляется побайтно в шестнадцатеричном виде с разделителем «.» или «:», например `00.45.f5.2d`.

Используя символ «,» в указателе диапазона, можно перечислить несколько непересекающихся диапазонов, объединив их в одном операнде. Например, выражение `tcp[2,10,13-16] == 00.01.c0.f8.01.66` сравнивает в заголовке протокола TCP поле «Тип обслуживания» с «0x00», поле «Протокол» с «0x01» и поле «IP-адрес источника» с «0xc0f80166».

ВЫПОЛНИТЬ!

11. Отобразите ICMP-ответы, используя в выражении фильтрации операнд «frame» с указателем диапазона.

При создании выражения фильтрации имейте в виду, что в буфере могут находиться кадры других узлов.

Укажите результирующее выражение фильтрации с необходимыми пояснениями. После просмотра результата для отображения пакетов без фильтрации нажмите кнопку «Clear» в строке фильтра.

Быстро вернуться к тому или иному ранее вводимому выражению фильтрации можно с помощью списка истории ввода, доступ к которому осуществляется нажатием на кнопку с символом «▼», расположенную в строке фильтра (не забывайте нажимать кнопку «Apply» для применения того или иного фильтра к буферу кадров).

1.5. Поиск кадров

Поиск кадров в буфере, удовлетворяющих тем или иным критериям, осуществляется с помощью команды меню ***Edit ⇒ Find Packet***. Диалоговое окно определения критериев поиска пакетов изображено на рис. 1.4.

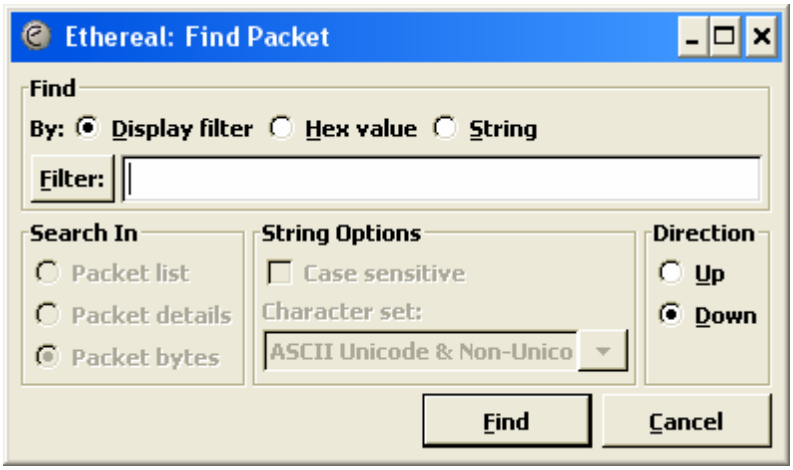


Рис. 1.4. Диалоговое окно определения критериев поиска кадров

Критерии поиска можно определять в виде выражения фильтрации (Display filter), шаблона в шестнадцатеричном виде (Hex value) и текстовой строки (String) в кодировке ASCII и (или) Unicode. В первом случае можно использовать все допустимые выражения фильтрации (табл. 1.1) и их логические комбинации. Во втором случае указывается шаблон для поиска в шестнадцатеричном коде. Поиск в строке может осуществляться в области общей информации о пакете (Packet list), в панели декодера протоколов (Packet details) и непосредственно в самом пакете (Packet bytes). Поиск может производиться вверх или вниз по списку пакетов (Direction).

Команды меню ***Edit ⇒ Find Next*** и ***Edit ⇒ Find Previous*** используются для поиска с заданными критериями следующего или предыдущего пакета соответственно.

ВЫПОЛНИТЬ!

12. Найдите все пакеты с помощью выражения фильтрации «`icmp.type==0`».
13. Найдите все пакеты по строке «reply» в области общей информации о пакете.
14. Найдите все пакеты по строке «reply» в панели декодера протоколов.
15. Проанализируйте результаты при разных вариантах поиска и дайте им объяснение.

1.6. Выделение ключевых кадров

В списке буфера ключевые или наиболее важные для дальнейшего анализа пакеты можно помечать с помощью команды ***Edit ⇒ Mark Packet*** (toggle) основного меню или команды Mark Packet (toggle) контекстного меню. Эта возможность полезна при дальнейшем поиске таких пакетов в большом буфере, так как они выделяются другим цветом, а также при сохранении, экспортировании и печати пакетов.

Информация о маркированных пакетах нигде не сохраняется, поэтому все маркеры будут потеряны при выгрузке файла данных.

ВЫПОЛНИТЬ!

16. Пометьте первый и последний пакеты, относящиеся к функционированию команды Ping.

1.7. Сохранение данных захвата

Сохранение данных в файле производится из меню ***File ⇒ Save*** или ***File ⇒ Save As***. Диалоговое окно сохранения данных изображено на рис. 1.5.

Обратите внимание, что сохранить можно все пакеты (All packets), только отображаемые (Displayed), выбранный пакет (Selected packet only), ранее маркированные с помощью основного или контекстного меню (Marked packet only и From first to last marked packet) или указанный диапазон пакетов (Specify a packet range). По умолчанию Ethereal сохраняет данные в файле типа Libpcap, совместимом по формату с файлами программы TcpDump, но путем указания определенного формата в строке ввода «File Type» этого диалогового окна данные захвата можно сохранять для экспорта в другие программы анализа трафика (около двадцати поддерживаемых в настоящее время форматов).

Не забывайте сохранять данные, прежде чем начинать другой сеанс записи.

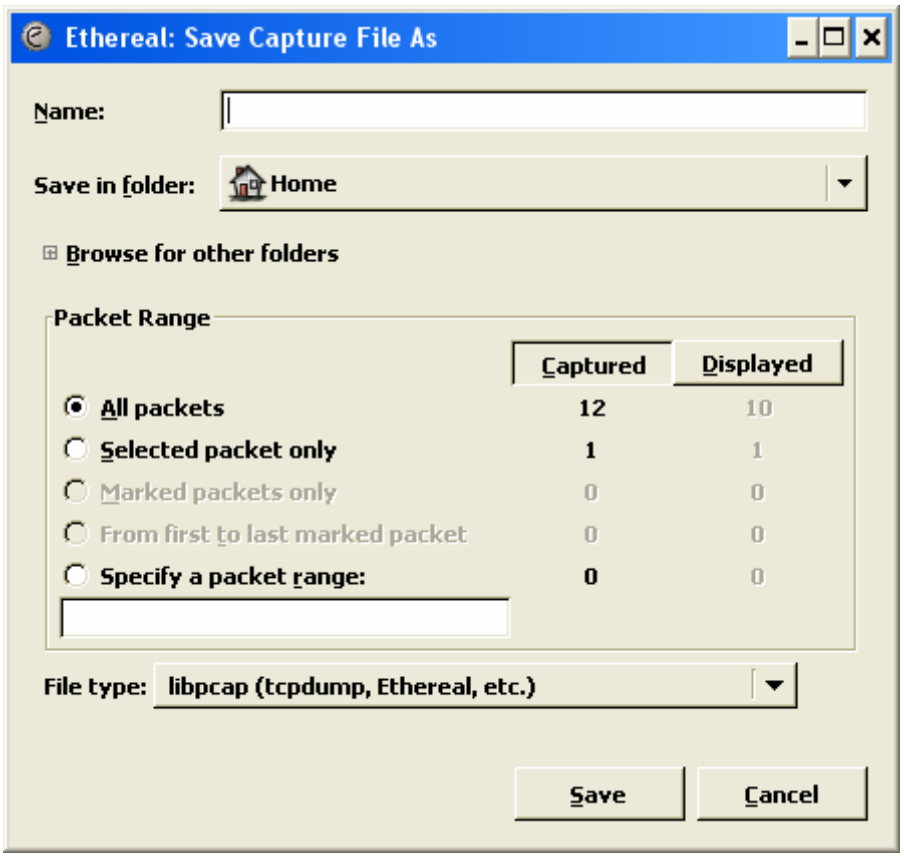


Рис. 1.5. Диалоговое окно сохранения данных

ВЫПОЛНИТЬ!

17. Сохраните все захваченные кадры в файле с именем «arp-ping» в каталоге, предлагаемом программой по умолчанию.
18. Сохраните в файле с именем «ping» только трафик команды Ping.

1.8. Печать информации

Распечатка информации о том или ином пакете или их множестве осуществляется посредством выполнения команды Print основного или контекстного меню. Диалоговое окно печати данных изображено на рис. 1.6.

При печати есть возможность осуществить вывод в указанный файл (Output to file) в виде простого текста (Plain text), определив диапазон распечатываемых пакетов (Packet Range) и формат вывода информации (Packet Format). Опции панели «Packet Range» полностью идентичны опциям соответствующей панели диалогового окна сохранения данных. При определении формата вывода в панели «Packet Format» есть возможность включить общую характеристику пакета (информацию верхней панели основного окна — «Packet summary line»), информацию, отображаемую на панели декодера протоколов с той или иной степенью детализации (Packet details) и собственно сам пакет в шестнадцатеричном виде (Packet bytes).

ВЫПОЛНИТЬ!

19. Выберите указателем мыши в списке пакетов первый ICMP-запрос и сохраните в файле «1.txt» информацию о нем с максимально возможной детализацией всех заголовков в декодере протоколов.

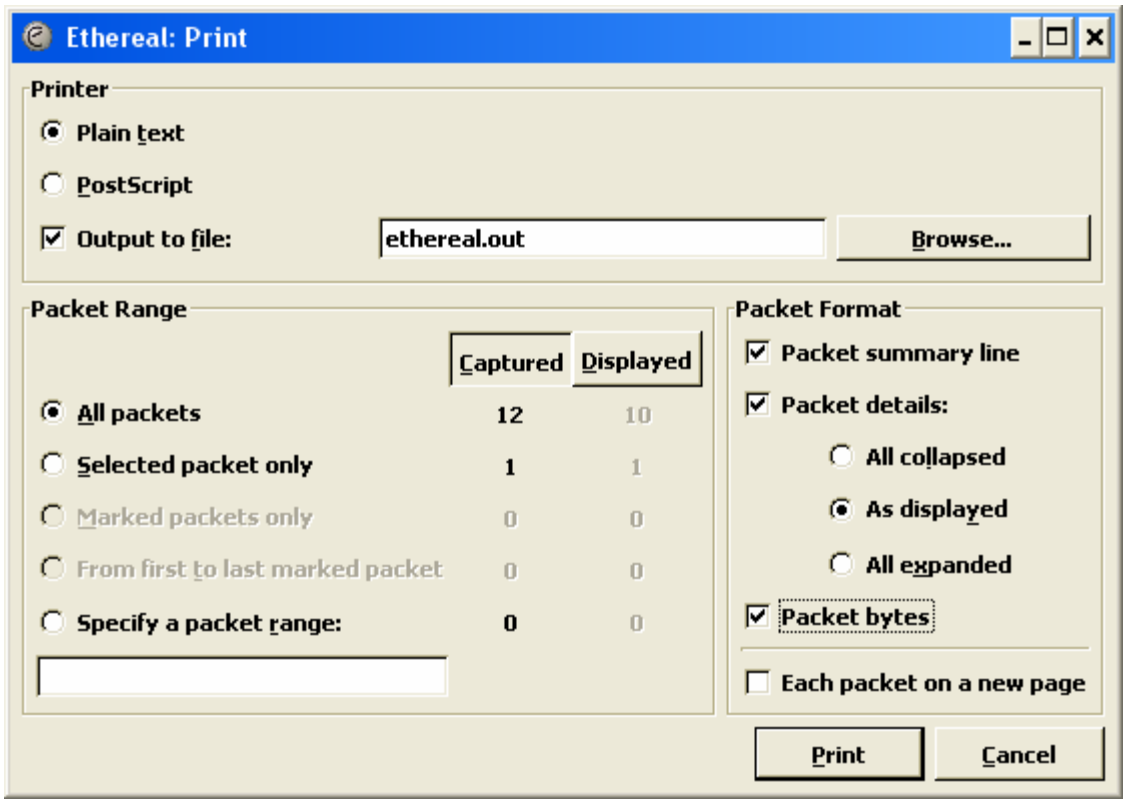


Рис. 1.6. Диалоговое окно печати данных

1.9. Просмотр кадра в отдельном окне

При составлении отчетов с использованием «скриншотов», а иногда и при анализе данных для просмотра двух пакетов одновременно удобно использовать возможность отображения пакета в отдельном окне.

Это реализуется с помощью команды «Show Packet in New Window» контекстного или основного меню программы «View». Окна, отображающие различные пакеты, показаны на рис. 1.7.

ВЫПОЛНИТЬ!

20. Пользуясь информацией об изображенных на рис. 1.7 пакетах, приведите обоснованные доводы, доказывающие их взаимосвязь.

1.10. Анализ протоколов Ethernet и ARP

При анализе протоколов Ethernet и ARP, которые находятся в иерархии протоколов ниже IP, для выключения отображения «лишней» информации на

панелях программы целесообразно отключить в программе анализ заголовка IP. Это реализуется с помощью команды «Enabled Protocols…» основного меню программы «Analyze». В диалоговом окне данной команды необходимо найти протокол IP, убрать соответствующий маркер, затем последовательно нажать кнопки «Apply» и «OK» (рис. 1.8).

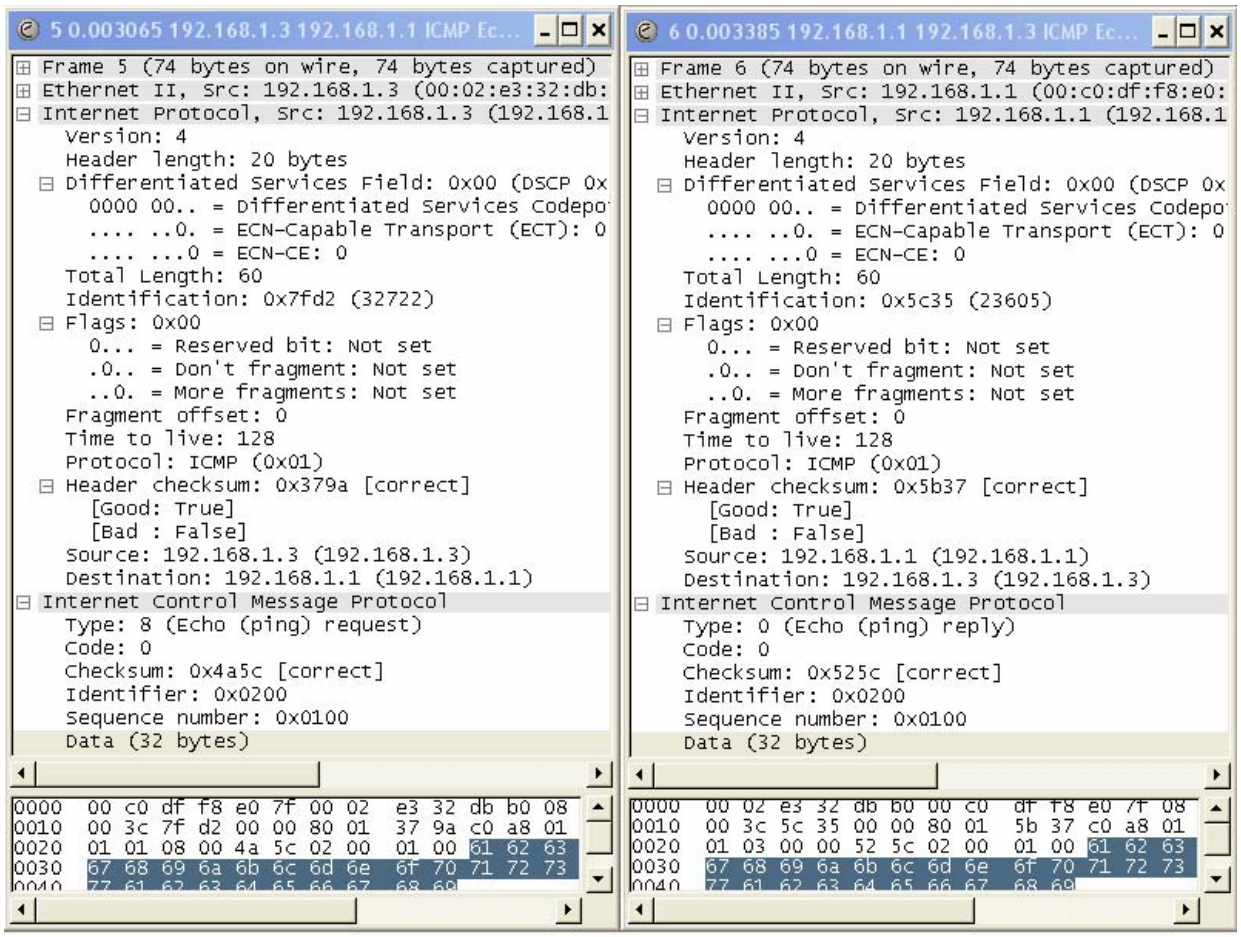


Рис. 1.7. Отображение пакетов в отдельных окнах

ВЫПОЛНИТЬ!

21. Отключите анализ заголовка IP.

В ряде случаев при отключении анализа заголовка IP отображаемые в списке буфера IP-адреса источника и получателя могут измениться!

22. Отобразите в отдельных окнах пакеты запроса и ответа протокола ARP и ответьте на следующие вопросы:
    a. Какое значение поля «тип протокола» в кадре Ethernet указывает на протокол ARP?
    b. По какому MAC-адресу отправлен запрос ARP?
    c. По какому MAC-адресу отправлен ответ ARP?
    d. Каким полем идентифицируются запрос и ответ ARP?
    e. В каких полях заголовка ARP передан запрос вашего узла?

f. В каких полях заголовка ARP передан ответ вашему узлу?

23. Загрузите созданный вами файл «1.txt» в редактор, допускающий выделение символов различным цветом.
24. Выделите различным цветом поля заголовка Ethernet в шестнадцатеричном представлении пакета.
25. Укажите, где находится поле контрольной суммы кадра Ethernet?
26. Захватите сетевой трафик вашего узла при обращении к стартовой странице поисковой системы Google и ответьте на следующие вопросы:
    a. Какие IP-адреса отображаются для узлов, участвующих в обмене по протоколу IP?
    b. Какие MAC-адреса имеют узлы, участвующие в обмене по протоколу IP?

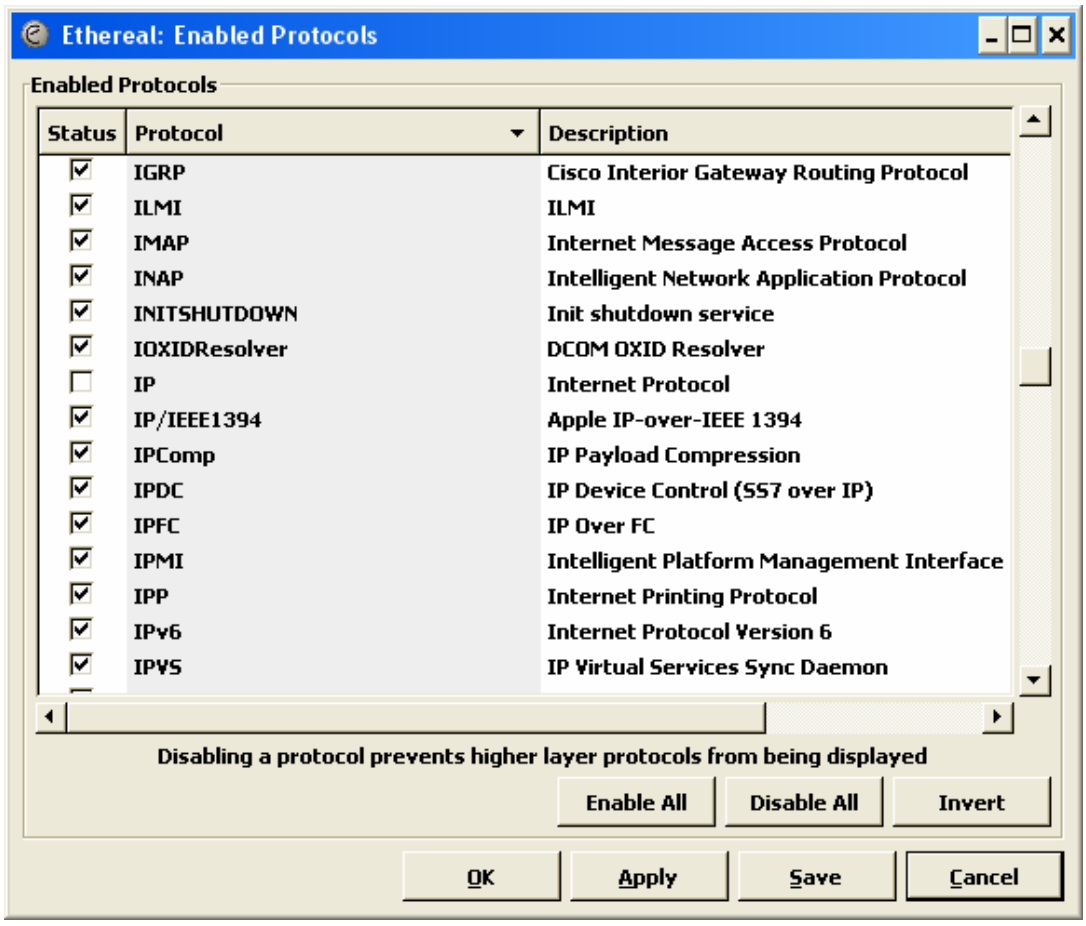


Рис. 1.8. Окно выбора протоколов для анализа

27. Включите анализ заголовка IP и ответьте на следующие вопросы:
    a. Какие IP-адреса отображаются для узлов, участвующих в обмене по протоколу IP?
    b. Какие MAC-адреса имеют узлы, участвующие в обмене по протоколу IP?
    c. Какой IP-адрес имеет узел с MAC-адресом, присутствующим во всех кадрах с протоколом IP? Какова роль этого узла?

1.11. Анализ протоколов IP и ICMP

ВЫПОЛНИТЬ!

28. Переключитесь в текстовый редактор и выделите различными цветами поля заголовка IP в шестнадцатеричном представлении пакета. Опишите назначение этих полей.
29. Загрузите созданный вами файл «ping». Сохраните два кадра «запрос — ответ» с требуемой детализацией для анализа полей ICMP и опишите назначение этих полей.
30. Проведите захват трафика команд Ping и PathPing при одинаковых значениях параметров -l и -n и проанализируйте различия в трафике этих команд.
31. Захватите сетевой трафик вашего узла при трассировке маршрута к поисковой системе Google (команда TraceRt) и ответьте на следующие вопросы:
    a. Почему MAC-адреса назначения и источника у всех кадров одинаковы и чьи это адреса?
    b. Почему узлы присылают ICMP сообщение «type 11»?
    c. Почему различные узлы присылают ICMP сообщение «type 11» на запрос к одному и тому же узлу?
    d. Сколько таких узлов, какие у них IP-адреса?
    e. Какова структура ICMP сообщения «type 11»?
    f. Какие поля ICMP одинаковы, а какие различны в последних трех запросах?
32. С помощью фильтра отобразите только ICMP-запросы. Приведите выражение фильтрации и объясните, почему выражения `icmp.type == 8` и `ip.src == X.X.X.X` (где `X.X.X.X` — IP-адрес вашего узла) не приводят к желаемому результату.
33. Ответьте на следующие вопросы:
    a. Каковы размеры кадров Ethernet, заголовков IP и сообщений ICMP, меняются ли они в процессе выполнения команды?
    b. Фрагментируются ли IP-дейтаграммы, передаваемые узлом?
    c. Какие поля заголовка IP меняются, а какие остаются неизменными в каждом пакете трафика?
    d. Какое поле заголовка IP изменяется в каждой тройке передаваемых кадров и для каких целей оно служит?
    e. Каким образом можно быстро определить число промежуточных маршрутизаторов на маршруте, если известно, что последний запрос, находящийся в буфере, достиг целевого узла?
34. С помощью фильтра отобразите только ICMP-сообщения, получаемые вашим узлом, и ответьте на следующие вопросы:
    a. Меняются ли в процессе выполнения команды размеры заголовков IP и сообщений ICMP? Чем можно объяснить данную ситуацию?

b. Имеются ли в буфере кадры, которые нельзя фрагментировать, и от какого узла они получены?

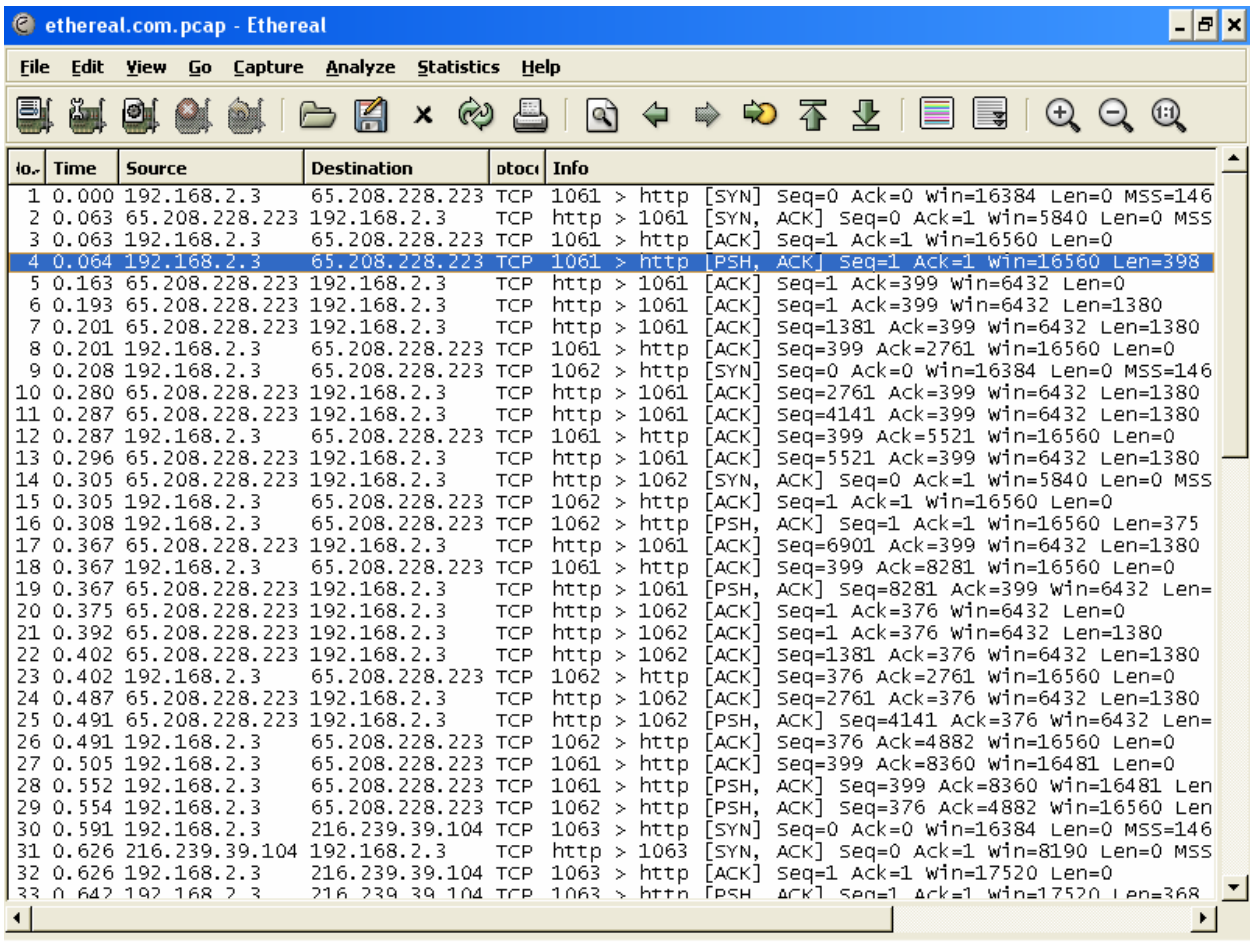
35. Захватите сетевой трафик функционирования команды Ping при проверке доступности сервера Google с параметром «r», равным 5. Сохраните данные в файле с именем «ping-r5». Ответьте на следующие вопросы:
    a. Поясните назначение параметра -r в команде Ping.
    b. Каким образом в кадрах передается информация о маршруте?
    c. Почему значение параметра -r в команде Ping не может быть больше 9?
    d. Каким образом ведут себя значения полей идентификатора и последовательного номера в заголовке ICMP захваченных кадров?
36. Захватите сетевой трафик функционирования команды Ping при проверке доступности сетевого узла вашего компьютерного класса с параметром «s», равным 4. Сохраните данные в файле с именем «ping-s4». Ответьте на следующие вопросы:
    a. Поясните назначение параметра -s в команде Ping.
    b. Каким образом в кадрах передается штамп времени?
    c. Почему значение параметра -s в команде Ping не может быть больше 4?
37. Захватите сетевой трафик функционирования команды Ping при проверке доступности сетевого узла вашего компьютерного класса с параметром «l», равным 3500, и «n», равным 1. Сохраните данные в файле с именем «ping3500». Ответьте на следующие вопросы:
    a. Сколько кадров передано и получено вашим узлом?
    b. Сколько IP-дейтаграмм передано и получено вашим узлом?
    c. Были ли IP-дейтаграммы подвергнуты фрагментации, какие поля заголовка IP указывают на это?
    d. Сколько фрагментов IP-дейтаграмм оказалось в буфере захвата?
    e. Какой размер исходной дейтаграммы, подвергнувшейся дефрагментации?
    f. Какие размеры разных фрагментов одной и той же дейтаграммы?
    g. Меняется ли идентификатор дейтаграммы в ее фрагментах, каково его значение?
    h. Какие поля заголовка IP предназначены для сборки исходной дейтаграммы из фрагментов в правильной последовательности?
    i. В каких фрагментах исходных дейтаграмм присутствует заголовок ICMP?
    j. Проанализируйте результаты и приведите схему обмена сообщениями ICMP между узлами.
38. С указанием значений всех необходимых полей заголовков покажите взаимосвязь кадров в рамках обмена «запрос — ответ» протокола ICMP.

1.12. Анализ протокола TCP

ВЫПОЛНИТЬ!

39. Захватите сетевой трафик при обращении к стартовой странице сервера www.ethereal.com. Для отображения в буфере кадров с протоколом TCP примените соответствующее выражение фильтрации.

В буфере захвата у вас находятся кадры, принадлежащие обмену клиента с сервером по протоколу HTTP, но в рамках текущего упражнения прикладной протокол нас не интересует, поэтому по аналогии с упражнением № 21 отключите анализ протокола HTTP. Фрагмент панелей со списком кадров после отключения анализа протокола FTP показан на рис. 1.9:



No.	Time	Source	Destination	Protocol	Info
1	0.000	192.168.2.3	65.208.228.223	TCP	1061 > http [SYN] Seq=0 Ack=0 Win=16384 Len=0 MSS=146
2	0.063	65.208.228.223	192.168.2.3	TCP	http > 1061 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS
3	0.063	192.168.2.3	65.208.228.223	TCP	1061 > http [ACK] Seq=1 Ack=1 Win=16560 Len=0
4	0.064	192.168.2.3	65.208.228.223	TCP	1061 > http [PSH, ACK] Seq=1 Ack=1 Win=16560 Len=398
5	0.163	65.208.228.223	192.168.2.3	TCP	http > 1061 [ACK] Seq=1 Ack=399 Win=6432 Len=0
6	0.193	65.208.228.223	192.168.2.3	TCP	http > 1061 [ACK] Seq=1 Ack=399 Win=6432 Len=1380
7	0.201	65.208.228.223	192.168.2.3	TCP	http > 1061 [ACK] Seq=1381 Ack=399 Win=6432 Len=1380
8	0.201	192.168.2.3	65.208.228.223	TCP	1061 > http [ACK] Seq=399 Ack=2761 Win=16560 Len=0
9	0.208	192.168.2.3	65.208.228.223	TCP	1062 > http [SYN] Seq=0 Ack=0 Win=16384 Len=0 MSS=146
10	0.280	65.208.228.223	192.168.2.3	TCP	http > 1061 [ACK] Seq=2761 Ack=399 Win=6432 Len=1380
11	0.287	65.208.228.223	192.168.2.3	TCP	http > 1061 [ACK] Seq=4141 Ack=399 Win=6432 Len=1380
12	0.287	192.168.2.3	65.208.228.223	TCP	1061 > http [ACK] Seq=399 Ack=5521 Win=16560 Len=0
13	0.296	65.208.228.223	192.168.2.3	TCP	http > 1061 [ACK] Seq=5521 Ack=399 Win=6432 Len=1380
14	0.305	65.208.228.223	192.168.2.3	TCP	http > 1062 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS
15	0.305	192.168.2.3	65.208.228.223	TCP	1062 > http [ACK] Seq=1 Ack=1 Win=16560 Len=0
16	0.308	192.168.2.3	65.208.228.223	TCP	1062 > http [PSH, ACK] Seq=1 Ack=1 Win=16560 Len=375
17	0.367	65.208.228.223	192.168.2.3	TCP	http > 1061 [ACK] Seq=6901 Ack=399 Win=6432 Len=1380
18	0.367	192.168.2.3	65.208.228.223	TCP	1061 > http [ACK] Seq=399 Ack=8281 Win=16560 Len=0
19	0.367	65.208.228.223	192.168.2.3	TCP	http > 1061 [PSH, ACK] Seq=8281 Ack=399 Win=6432 Len=
20	0.375	65.208.228.223	192.168.2.3	TCP	http > 1062 [ACK] Seq=1 Ack=376 Win=6432 Len=0
21	0.392	65.208.228.223	192.168.2.3	TCP	http > 1062 [ACK] Seq=1 Ack=376 Win=6432 Len=1380
22	0.402	65.208.228.223	192.168.2.3	TCP	http > 1062 [ACK] Seq=1381 Ack=376 Win=6432 Len=1380
23	0.402	192.168.2.3	65.208.228.223	TCP	1062 > http [ACK] Seq=376 Ack=2761 Win=16560 Len=0
24	0.487	65.208.228.223	192.168.2.3	TCP	http > 1062 [ACK] Seq=2761 Ack=376 Win=6432 Len=1380
25	0.491	65.208.228.223	192.168.2.3	TCP	http > 1062 [PSH, ACK] Seq=4141 Ack=376 Win=6432 Len=
26	0.491	192.168.2.3	65.208.228.223	TCP	1062 > http [ACK] Seq=376 Ack=4882 Win=16560 Len=0
27	0.505	192.168.2.3	65.208.228.223	TCP	1061 > http [ACK] Seq=399 Ack=8360 Win=16481 Len=0
28	0.552	192.168.2.3	65.208.228.223	TCP	1061 > http [PSH, ACK] Seq=399 Ack=8360 Win=16481 Len
29	0.554	192.168.2.3	65.208.228.223	TCP	1062 > http [PSH, ACK] Seq=376 Ack=4882 Win=16560 Len
30	0.591	192.168.2.3	216.239.39.104	TCP	1063 > http [SYN] Seq=0 Ack=0 Win=16384 Len=0 MSS=146
31	0.626	216.239.39.104	192.168.2.3	TCP	http > 1063 [SYN, ACK] Seq=0 Ack=1 Win=8190 Len=0 MSS
32	0.626	192.168.2.3	216.239.39.104	TCP	1063 > http [ACK] Seq=1 Ack=1 Win=17520 Len=0
33	0.642	192.168.2.3	216.239.39.104	TCP	1063 > http [PSH, ACK] Seq=1 Ack=1 Win=17520 Len=368

Рис. 1.9. Отображение информации о протоколе TCP

Обратите внимание, что теперь по каждому захваченному кадру приводится информация, касающаяся только протокола TCP. Например, для пакета № 4 (рис. 1.9) запись «1061> ftp» означает порты источника и назначения, «[PSH, ACK]» — установленные биты флагов, «Seq=1» — последовательный номер, «Ack=1» — номер подтверждения, «Win=16560» — размер приемного окна, «Len=398» — размер пересылаемого блока данных.

Каждая TCP-сессия (причем при обращении к одной странице сессий может быть несколько!) начинается с обмена тремя TCP-сегментами с установленными битами SYN, SYN-ACK и ACK. На рис. 1.9 можно видеть открытие трех сессий TCP (кадры с номерами 1, 2, 3; 9, 14, 15; 30, 31, 32 соответственно).

ВЫПОЛНИТЬ!

40. Определите количество сеансов TCP в буфере захваченных пакетов.

На рис. 1.9 также видно, что сеансы TCP начинаются с относительных последовательных номеров, равных нулю. Для того чтобы отобразить реальные последовательные номера, выбранные узлами при взаимодействии, необходимо выполнить команду меню ***Edit ⇒ Preferences***, в появившемся диалоговом окне (фрагмент диалогового окна см. на рис. 1.10) выбрать протокол TCP и убрать маркер в строке параметра «Relative sequence numbers and window scaling».

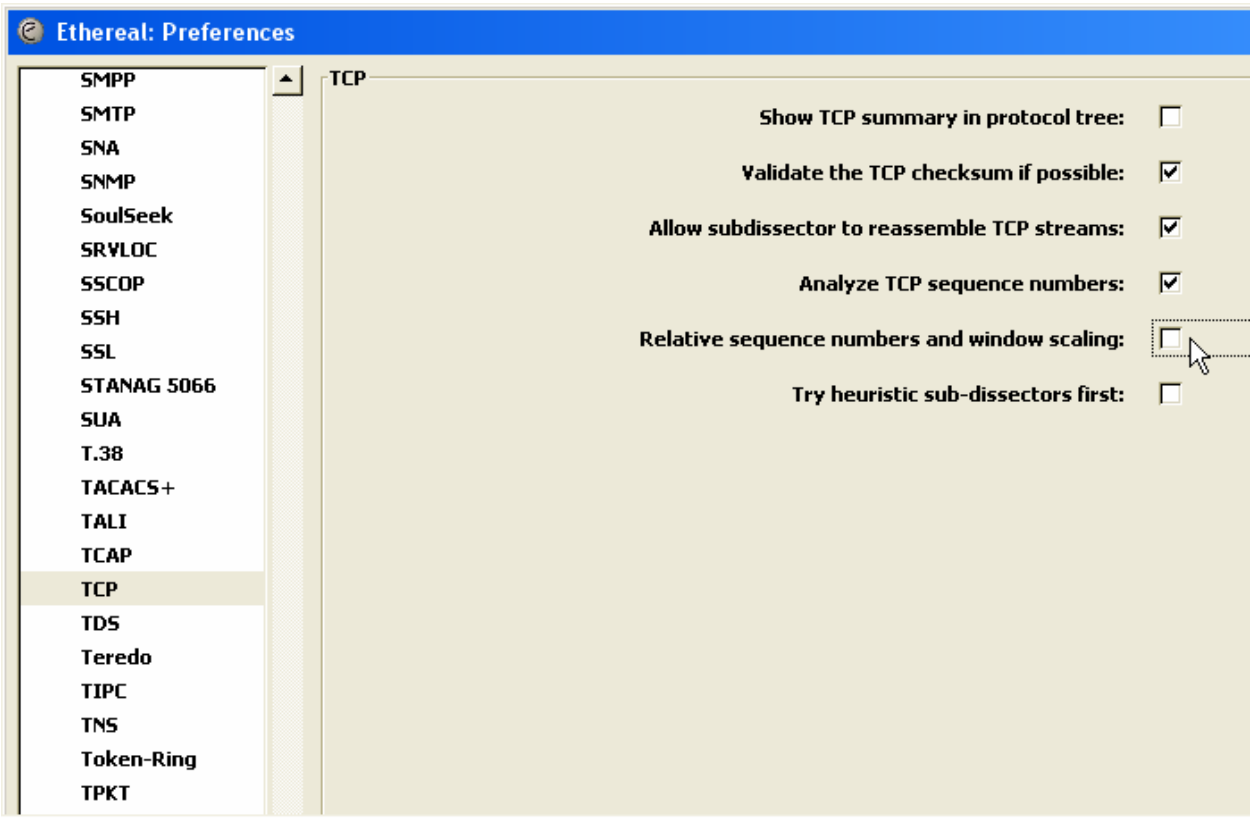


Рис. 1.10. Параметры анализа протокола TCP

ВЫПОЛНИТЬ!

41. Отобразите реальные последовательные номера в рамках сеансов TCP.
42. Проанализируйте третий кадр в рамках какого-либо сеанса TCP и ответьте на следующие вопросы:
    a. Какие порты используются клиентом и сервером?

b. Какой начальный последовательный номер выбран клиентом?
c. Присутствует ли в этом кадре поле подтверждения, каково его значение?
d. Какая длина заголовка TCP, присутствуют ли данные в этом кадре?
e. Какой бит флагов установлен и для чего он служит?
f. Какие дополнительные опции TCP передаются клиентом в этом кадре?
g. Сохраните кадр и выделите различным цветом поля заголовка TCP, пояснив их назначение.

Немаловажная возможность программы Ethereal по анализу TCP трафика состоит в том, что с помощью команды меню ***Statistics ⇒ Conversations*** можно быстро определить все сеансы, имеющиеся в буфере. В диалоговом окне для отображения сеансов TCP необходимо выбрать закладку TCP (рис. 1.11).

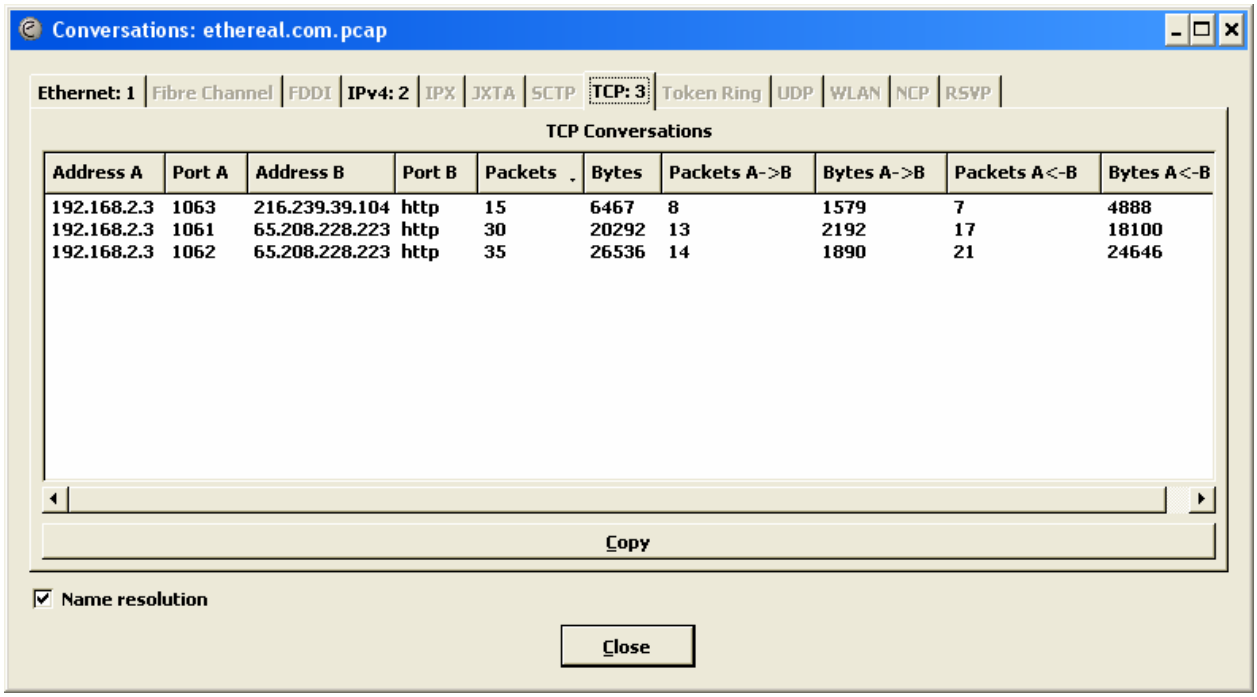


Рис. 1.11. Статистика по сеансам TCP

ВЫПОЛНИТЬ!

43. Отобразите статистику сеансов TCP.
44. Выберите первый сеанс и с помощью контекстного меню ***Apply as Filter ⇒ Selected ⇒ A<—>B*** отобразите в буфере кадры, принадлежащие этому сеансу.

Для того чтобы быстро просмотреть передаваемые данные в рамках того или иного сеанса, используют команду меню Analyze ⇒ Follow TCP Stream. После выполнения команды на экране появится диалоговое окно, в котором

разными цветами будут отображены как запросы клиента, так и ответы сервера (рис. 1.12).

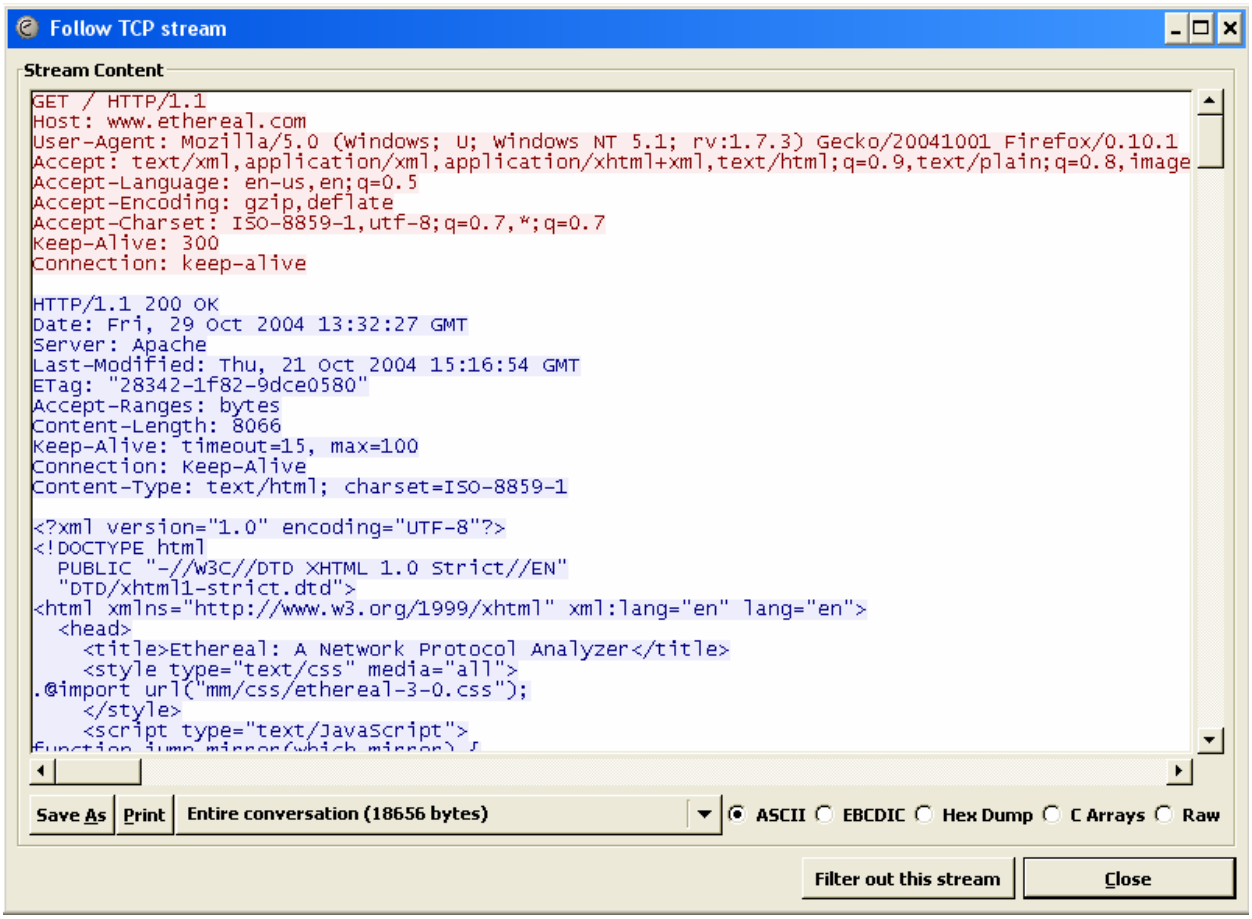


Рис. 1.12. Восстановленный сеанс TCP

Кнопка «Entire conversation» с раскрывающимся списком позволяет отобразить обе стороны, участвующие в обмене, или только одну из них. Диалоговое окно позволяет отобразить данные в различных форматах (ASCII, EBCDIC, Hex Dump, C Arrays, Raw) и сохранить их в файл. При обнаружении в сеансе кадров с каким-либо файлом можно отобразить лишь поток соответствующего направления, выбрать необходимый формат и сохранить его на диск.

ВЫПОЛНИТЬ!

45. Определите, что передавалось в рамках захваченных вами сеансов TCP.